REMARKS

I. Introduction

In response to the Office Action dated January 27, 2005, claim 6 has been amended. Claims 1-37 remain in the application. Re-examination and re-consideration of the application, as amended, is requested.

II. Allowable Subject Matter

In paragraph 7, the Office Action indicates that the subject matter of claims 12-15 and 36-37 would be allowable if written in independent form including all of the limitations of the base claim and any intervening claims. The Applicants acknowledge the Office Action's indication of allowable subject matter, but traverse the rejection of claims 1-11 and 16-35.

III. The Cited References and the Subject Invention

A. The Maillard Reference

U.S. Patent No. 6,466,671, issued October 15, 2002 to Maillard et al. disclose a smartcard for use with a receiver of encrypted broadcast signals, and receiver. A smartcard for use with a receiver of encrypted broadcast signals comprises a microprocessor for enabling or controlling decryption of said signals. A memory is coupled to the microprocessor. The microprocessor is adapted to enable or control the individual decryption of a plurality of such signals from respective broadcast suppliers of such signals by means of respective dynamically created zones in the memory, the dynamically created zones each being arranged to store decryption data associated with a respective one of said broadcast suppliers.

B. The Saito Reference

European Patent Application EP 1122910 discloses a method and an apparatus allowing to ensure protecting digital data. In addition to re-encrypting the data by using an unchangeable key, the data is double re-encrypted by using a changeable key. The changeable key is used first and the unchangeable key is then used, or in another case, the unchangeable key is used first, and the changeable key is then used. In the aspect of embodiments, there is a case adopting a software, a case adopting a hardware, or a case adopting the software and the hardware in combination. The

hardware using the unchangeable key developed for digital video is available. In adopting the software, encryption/decryption is performed in a region below the kernel where the user cannot handle to ensure the security for the program and for the key used. More concretely, encryption/decryption is performed in a filter driver, a device driver, i.e., a disk driver and a network driver, in an I/O manager and an RTOS using a HAL. Either one of two filter drivers, with a file system driver between them, may be used and further, both of them may be used.

C. The Lee Reference

U.S. Patent No. 5,790,783, issued August 4, 1998 to Lee et al. discloses Method and apparatus for upgrading the software lock of microprocessor. When a processor upgrade occurs, software that was serialized to the previously installed processor detects that it is running on an unauthorized processor. The software initiates a reauthorization process based on a reauthorization use profile. The temporary re-enabling of the software is allowed if the authorization service is not available.

IV. Office Action Prior Art Rejections

In paragraphs (5)-(6), the Office Action rejected claims 1-11 and 16-35 under 35 U.S.C. § 103(a) as unpatentable over Maillard et al., U.S. Patent No. 6,466,671 (Maillard) in view of Saito, EP 1122910 A1 (Saito), and further in view of Lee et al., U.S. Patent No. 5,790,783 (Lee).

With Respect to Claims 1-2, 16, 23-26: Claim 1 recites:

A method of storing program material for subsequent replay, comprising the steps of:

receiving a data stream in a receiver having a storage device, the data stream comprising the program material encrypted according to a first encryption key and control data, the control data comprising the first encryption key and being encrypted;

further encrypting the encrypted program material according to a second encryption key;

encrypting the second encryption key according to a third encryption key to produce a fourth encryption key; and

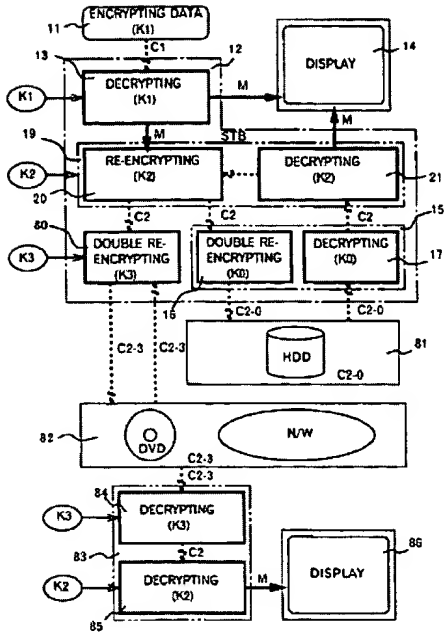
storing the further encrypted program material and control data and the fourth encryption key in the storage device.

According to the Office Action, Saito

"discloses a method and device for protecting digital data by double re-encryption comprising double encrypting the digital video program (Fig. 8, elements 20 and 16) and storing the encrypted program material and control data and the fourth decryption key in the storage device (Fig. 8, element 81)"

as follows:

FIG. 8



The Office Action is correct in that the foregoing teaches double re-encryption. However, claim 1 recites that the received (encrypted) data stream is *further encrypted.* The Saito reference teaches the opposite. The received data stream is decrypted by block 13, re-encrypted by block 20 and double-re-encrypted by block 80. Saito, in fact, teaches away from the Applicant's invention.

According to the Office Action, it would have been obvious to one of ordinary skill in the art to combine the Maillard and Saito references to better protect the program material. The Applicants respectfully disagree. Maillard does not teach the local storage of program material for later viewing at all.

The Office Action acknowledges that even when combined, Maillard and Saito do not disclose encrypting the second key according to a third key to produce a fourth encryption key, but assert that the Lee reference does so. The Lee reference, however, is directed at the encryption of an unchangeable microprocessor serial number. This is not analogous to the secure storage of copyrighted program material for later replay.

The Saito reference also teaches away from Lee. Saito teaches a particular double encryption technique that is directed to solve the problem of where and how to store the key used to encrypt

the program material. Saito teaches that this problem is solved by using double encryption and symmetric use of a changeable and unchangeable key.

In Fig. 1, reference numeral 1 represents the digital data supplied by broadcasting means such as digital terrestrial wave broadcasting, digital CATV broadcasting, digital satellite broadcasting, etc., by network means such as Internet, or by a digital storage medium such as a DVD, a CD, etc. The data is encrypted by using a first changeable key K1 to prevent illegitimate use:

$$C1=E(M, K1)$$

and is supplied to a set-top box 2.

When the encrypted digital data C1 is supplied to the set-top box 2, the encrypted digital data C1 is decrypted at a decryption unit 3 by using the first changeable key K1 obtained from a key center via the same route as or via a different route from that of the encrypted digital data C1:

$$M=D(C1, K1)$$

and data M thus decrypted is outputted to a display unit 4 or the like.

In a case where the decrypted data M is stored in a medium such as a digital video disk (DVD) RAM or a hard disk, etc., or it is transferred outside via a network, the decrypted data M is re-encrypted at an encryption unit 6 of an unchangeable key encryption/decryption unit 5 by using an unchangeable key K0: and re-encrypted data C0 is stored in or transferred to an external device 8.

In a case where the re-encrypted data C0 is used again, the re-encrypted data C0 read from a storage medium of the external device 8 or transferred via the network is re-decrypted by using the unchangeable key K0 at a decryption unit 7 of the unchangeable key encryption/decryption unit 5: and the decrypted data M is outputted to the display unit 4 or the like.

In this case, in order to ensure security, it may be arranged in such a manner that the re-encrypted data C0 in the storage medium is erased when the re-encrypted data C0 is read from the storage medium via a route shown by a broken line in the figure and that the data re-encrypted again by using the unchangeable key K0 is re-stored.

In USP 5,805,706, an integrated circuit for performing re-encryption/re-decryption is described.

In the set-top box as arranged above, it is easy to handle because re-encryption/re-decryption is automatically carried out by the hardware by using the unchangeable key K0, and it is effective for forcible re-encryption/re-decryption of the digital data, which must be protected.

However, as the unchangeable key K0 is placed in the device, and there is possibility that the unchangeable key K0 may be known to others, it may become impossible to protect the digital data thereafter.

To solve the above problem, present invention provides a method and an apparatus for double re-encrypting the data by using a changeable key in addition to re-encrypting by using an unchangeable key.

In use of the unchangeable key and the changeable key, there are cases where the changeable key is used first and the unchangeable key is then used, and where the unchangeable key is used first and the changeable key is then used.

The key used first when re-encrypting is used finally when decrypting, and accordingly, even if data, which is subsequently re-encrypted, is cryptanalyzed, security is highly ensured. Therefore, in a case where a changeable key is used first and next, an

unchangeable key is used for re-encryption, the possibility that the changeable key is known to others is very low even when the unchangeable key has been known to the others. (page 3, line 54 - page 4, line 53, emphasis added).

Not only is there no teaching to combine Maillard and Saito, Saito itself teaches away from any combination with Lee. "A reference may be said to teach away when a person of ordinary skill, upon reading the reference, would be discouraged from following the path set out in the reference, or would be led in a direction divergent from the path that was taken by the applicant. The degree of teaching away will of course depend on the particular facts; in general, a reference's disclosure will teach away if it suggests that the line of development flowing from the reference's disclosure is unlikely to be productive of the result sought by the Applicant. *In re Gurley*, 27 F.3d 551, 553, 31 U.S.P.Q.2d 1130 (Fed. Cir. 1994).

For all of the foregoing reasons, the Applicants respectfully traverse the rejection of claim 1.

Claim 2 recites the features of claim 1 and is patentable for analogous reasons. Claim 2 also recites associated features (e.g. decrypting the further encrypted program material with the second key, and decrypting the encrypted program material with the first key).

Claim 16 likewise recites a first encryption module that is not disclosed in the cited references.

Claims 23-26 also recite further encryption of the received datastream, features that are not disclosed or taught by the cited references. These claims are patentable over the cited references as well.

With Respect to Claims 3, 19-20, and 27: Claim 3 recites accepting a PPV request before decrypting the encrypted program material using the first encryption key. According to the Office Action, this is disclosed in the Maillard reference as follows:

> In an eighth aspect, the present invention provides a receiver/decoder for receiving and decrypting broadcast signals in a Pay Per View (PPV) mode, the receiver/decoder comprising means for detecting control signals which enable or control the decryption of particular program transmissions within said broadcast signals, said control signals including information identifying each transmission in a series of transmissions of the same program, and limiting means coupled to said detecting means for limiting the number of transmissions in said series which can be decrypted. (col. 3, lin3s 57-67)

However, the foregoing refers to operations that are performed on the received datastream. Claim 3 instead refers to operations that are performed after the program material is stored and playback. The combined references of record would teach one of ordinary skill in the art to decrypt

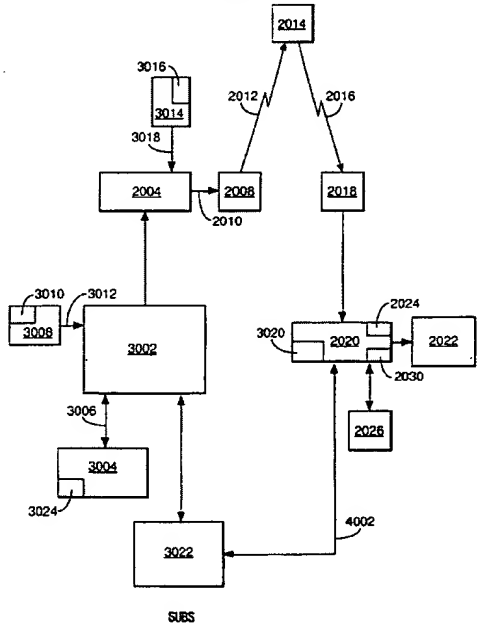
the program material (as described in the Maillard reference), re-encrypt it (perhaps twice, as described in Saito), and store it. Upon playback, the retrieved program material would be decrypted (perhaps twice as described in Saito), but not with the first key that was used in the transmission of the program material as that encryption was already decoded completely before storage. Claims 19, 20, and 27 are patentable for analogous reasons.

With Respect to Claims 4 and 28: Claim 4 recites:

> *The method of claim 2, further comprising the steps of:*
> *further encrypting the control data according to the second encryption key;*
> *storing the further encrypted control data; and*
> *decrypting the further encrypted control data according to the second encryption key.*

According to the Office Action, this is disclosed in the Maillard reference as follows:

Fig.2.



Without further explanation, the Applicants are unable to determine how FIG. 2 discloses further encrypting the *control data* according to the second encryption key and storing it. Accordingly, the Applicants respectfully traverse.

Claim 28 is patentable for analogous reasons.

With Respect to Claim 6-7, 21, and 30-31: Claim 6 recites that the second key is unique to the receiver. According to the Office Action the combination of the references disclose this feature.

However, the Office Action does not indicate where this feature is found in any one of the references. Without further guidance, the Applicants respectfully traverse.

"If when combined, the references 'would produce a seemingly inoperative device,' then they teach away from their combination." *In re Gurley*, 27 F.3d 551, 553, 31 U.S.P.Q.2d 1130 (Fed. Cir. 1994) (quoting *In re Sponnoble*, 405 F.2d 578, 587, 160 U.S.P.Q. 237, 244 (C.C.P.A. 1969).

When combined, the references actually teach away from the Applicants' invention. For example, the combined references would teach [WHAT THE COMBINED REFERENCES TEACH].

The various elements of the Applicants' claimed invention together provide operational advantages over the systems disclosed in Maillard, Saito, and Lee. In addition, Applicants' invention solves problems not recognized by Maillard, Saito, and Lee.

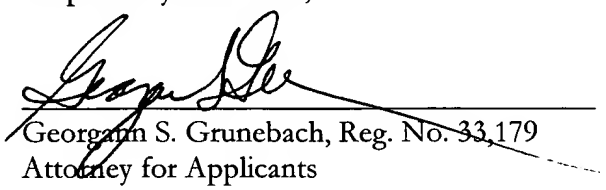
V. Dependent Claims

Dependent claims 2-15, 17-22, and 26-37 incorporate the limitations of their related independent claims, and are therefore patentable on this basis. In addition, these claims recite novel elements even more remote from the cited references. Accordingly, the Applicants respectfully request that these claims be allowed as well.

VI. Conclusion

In view of the above, it is submitted that this application is now in good order for allowance and such allowance is respectfully solicited. Should the Examiner believe minor matters still remain that can be resolved in a telephone interview, the Examiner is urged to call Applicants' undersigned attorney.

Respectfully submitted,



Georgann S. Grunebach, Reg. No. 33,179
Attorney for Applicants

Date: April 25, 2005

The DIRECTV Group, Inc.
RE / R11 / A109
P.O. Box 956
2250 E. Imperial Highway
El Segundo, CA 90245-0956

Phone: (310) 964-0735